IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

BRITTANY MAY, ERIKA RANCK, LAUREN TURNER, and STEPHEN THOMAS, on behalf of themselves and all others similarly situated, Plaintiffs, v. FIVE GUYS ENTERPRISES, LLC, Defendant.	Case No.: 1:23-cv-00029 **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Brittany May, Erika Ranck, Lauren Turner, and Stephen Thomas ("Plaintiffs") bring this Class Action Complaint against Five Guys Enterprises, LLC ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of Defendant's job applicants and current and former employees, including, but not limited to, name and Social Security number.

2. According to Defendant's website, it operates 1,700 hamburger restaurants worldwide.[2]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.
[2] *See* https://www.fiveguys.com/the-five-guys-story (last visited Jan. 5, 2023).

3. Prior to and through September 17, 2022, Defendant obtained the PII of Plaintiffs and Class Members, including by collecting it directly from Plaintiffs and Class Members.

4. Prior to and through September 17, 2022, Defendant stored the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

5. On or before September 17, 2022, Defendant learned of a data breach on its network that occurred on or around September 17, 2022 (the "Data Breach").

6. Defendant determined that, during the Data Breach, an unknown actor accessed files containing the PII of Plaintiffs and Class Members.

7. On or around December 29, 2022, Defendant began notifying various states Attorneys General of the Data Breach.

8. On or around December 29, 2022, Defendant began notifying Plaintiffs and Class Members of the Data Breach.

9. On or around February 5, 2023, reports began surfacing on the Internet that the Data Breach resulted from a ransomware attack undertaken by the "ALPHV/Blackcat" ransomware group and that the attacker had posted information exfiltrated during the attack on the dark web.

10. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that may have been accessed and/or acquired by an unauthorized actor included name and Social Security number.

11. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs

and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

12. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited more than three months after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

13. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

14. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

15. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the

actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

16. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

17. Plaintiff May is a citizen of Florida residing in North Fort Myers, Florida.

18. Plaintiff Ranck is a citizen of Virginia residing in Virginia.

19. Plaintiff Turner is a citizen of California residing in Los Angeles, California.

20. Plaintiff Thomas is a citizen of Texas residing in Texas.

21. Defendant is a Virginia corporation with a principal place of business in Lorton, Virginia.

22. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently

unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

23. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiffs, is a citizen of a state different from Defendant to establish minimal diversity.

25. Under 28 U.S.C. § 1332(d)(10), Defendant is a citizen of Delaware and Virginia because it is a limited liability company formed under Delaware law with its principal place of business in Lorton, Virginia.

26. The Eastern District of Virginia has personal jurisdiction over Defendant because it conducts substantial business in Virginia and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

27. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

28. Defendant collected the PII of Plaintiffs and Class Members, including Defendant's

job applicants and current and former employees.

29. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

30. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

31. On or about December 29, 2022, Defendant sent Plaintiffs and Class Members a notice of the Data Breach (the "Notice of Data Breach"). Defendant informed Plaintiffs and other Class Members that:

> Five Guys Enterprises, LLC ("Five Guys") understands the importance of protecting the information that we maintain. We are writing to inform you that we recently identified and addressed a security incident that may have involved your information. This letter explains the incident, measures we have taken, and some steps you may choose to take.
>
> We identified a security incident on September 17, 2022 that involved unauthorized access to files on a file server. We immediately implemented our incident response plan, took steps to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations was engaged. We also notified law enforcement and are supporting its investigation.
>
> The investigation identified unauthorized access to files on our file server that occurred on September 17, 2022. We conducted a careful review of those files and, on December 8, 2022, determined that the files contained information submitted to us in connection with the employment process, including your name and Social Security number.[3]

[3] Exhibit 1 (sample Notice of Security Incident filed with Montana Attorney General).

32. The Notice of Data Breach that Defendant sent to Plaintiffs stated that Plaintiffs' names and Social Security numbers were impacted during the Data Breach.

33. Defendant admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members, including name and Social Security number.

34. In response to the Data Breach, Defendant claims that it "immediately implemented our incident response plan, took steps to contain the activity, and launched an investigation."[4]

35. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

36. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

38. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

39. In the years immediately preceding the Data Breach, Defendant knew or should

[4] *Id.*

have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

40. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[5]

41. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[6]

42. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[7]

---

[5] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

[6] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[7] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

43. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

44. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

45. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

46. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members.

47. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members.

48. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

49. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely

maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

51. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

52. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

[9] *Id.* at 3-4.

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[10]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

54. Given that Defendant was storing the PII of individuals who had applied for jobs during the decade or more prior to the Data Breach, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

55. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of individuals who had applied for jobs during the decade or more prior to the Data Breach, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

56. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

57. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

60. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

61. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200,

[12] 17 C.F.R. § 248.201 (2013).

[13] *Id*.

and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

63. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[17]

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

years.

66. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

67. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

68. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

69. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

70. To date, Defendant has offered Plaintiffs and Class Members only one year of credit monitoring and identity protections services through IDX. The offered service is inadequate to

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

71. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Plaintiff May's Experience

72. Plaintiff May applied for a job with Defendant and ceased working for Defendant approximately ten years prior to the Data Breach and received Defendant's Notice of Data Breach, dated December 29, 2022, on or about that date. The notice stated that Plaintiff May's personal information, including name and Social Security number, were impacted by the Data Breach.

73. As a result of the Data Breach, Plaintiff May's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff May's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff May will have to worry about when and how her sensitive information may be shared or used to her detriment.

74. As a result of the Data Breach notice, Plaintiff May spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

75. Additionally, Plaintiff May is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

76. Plaintiff May stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and

passwords for her various online accounts.

77. Plaintiff May suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

78. Plaintiff May has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

79. Plaintiff May has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ranck's Experience

80. Ms. Ranck is a Data Breach victim, receiving Defendant's Breach Notice in early January 2023.

81. Ten years ago, Ms. Ranck was employed by Five Guys for 2-3 months.

82. Ms. Ranck does not recall ever learning that her information was compromised in a data breach incident, other than the breach at issue in this case.

83. When she was seeking employment with Five Guys, Five Guys requested she provide her PII to it as a condition of her employment.

84. Ms. Ranck trusted Five Guys would use reasonable measures to protect her PII according to Defendant's internal policies, as well as state and federal law. She complied with its request and provided her PII to Five Guys. Indeed, she viewed reasonable data protection as implicit in her agreement to provide her PII to Five Guys in return for paid employment.

85. Ms. Ranck received a Breach Notice on January 3, 2023, indicating that her PII,

including at least her name and Social Security number, was compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Ms. Ranck to be at a substantial risk for further identity theft.

86. In fact, because Five Guys failed in its duties, Ms. Ranck has suffered repeated fraud. Her name and credit are being used to open multiple accounts.

87. On January 5, 2023, Ms. Ranck received an email from U-Haul's collections department stating she owes U-Haul $118.05 from a reservation made on December 2, 2022 fraudulently made in her name. Ms. Ranck did not make any reservation with U-Haul in December 2022.

88. Additionally, for the last several months, Ms. Ranck has received notifications from a Walmart+ account fraudulently associated with her phone number, name, email address, and home address.

89. As a result of the Data Breach and the recommendations of Defendant's Breach Notice, Ms. Ranck made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, and monitoring her credit information as suggested by Five Guys.

90. Ms. Ranck has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. In fact, she has devoted over two full workdays to addressing the ramifications of the Data Breach. Ms. Ranck fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Ms. Ranck has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and

harm to a Data Breach victim that the law contemplates and addresses.

91. Ms. Ranck is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing its current, former, and prospective employees about the Data Breach.

92. Ms. Ranck has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Turner's Experience

93. Plaintiff Turner supplied PII to Five Guys in connection with a job application. She was an employee with Five Guys for in or around 2011.

94. On or around December 29, 2022, over a decade after working for Five Guys, Plaintiff Turner received a Notice of Data Breach, which stated her personal information, including her name and Social Security number, were impacted by the data breach.

95. Plaintiff Turner has seen a marked increase in spam emails, texts, and phone calls since around the time of the September 2022 breach.

96. As a result of the Data Breach, Plaintiff Turner's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Turner's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Turner will have to worry about when and how her sensitive information may be shared or used to her detriment.

97. As a result of the Data Breach notice, Plaintiff Turner spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice

of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

98. Additionally, Plaintiff Turner is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

99. Plaintiff Turner stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

100. Plaintiff Turner suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

101. Plaintiff Turner has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

102. Plaintiff Turner has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

103. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

104. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach

that Defendant sent to Plaintiffs and Class Members on or around December 29, 2022 (the "Nationwide Class").

105. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

> All individuals who applied for a job with or were employed by Defendant on or before September 17, 2022, and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 29, 2022 (the "Employee Subclass") (collectively, with the Nationwide Class, "the Classes").

106. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff May asserts claims on behalf of a separate subclass, defined as follows:

> All Florida residents whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 29, 2022 (the "Florida Subclass").

107. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Ranck asserts claims on behalf of a separate subclass, defined as follows:

> All Virginia residents whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 29, 2022 (the "Virginia Subclass").

108. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Turner asserts claims on behalf of a separate subclass, defined as follows:

> All California residents whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 29, 2022 (the "California Subclass") (collectively, with the Nationwide Class, the Florida Class, and the

Virginia Class, "the Classes").

109. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

110. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

111. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant reported to the Massachusetts Attorney General that 93 residents of Massachusetts were impacted in the Data Breach and reported to the Montana Attorney General that 12 residents of Montana were impacted in the Data Breach, and the Classes are apparently identifiable within Defendant's records. The total number of impacted individuals is expected to be significant as Defendant operates 1,700 restaurants and the Data Breach impacted individuals who had applied for jobs during the decade or more prior to the Data Breach.

112. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members

to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

113. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

114. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

115. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

116. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

117. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

118. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

119. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

120. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act

unlawfully as set forth in this Complaint.

121. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

123. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

124. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

125. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

126. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

127. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

128. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

129. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiffs' and the Nationwide Class's confidential PII in the course of its business practices.

130. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

131. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

132. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

133. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

134. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in,

and possibly remains in, Defendant's possession.

135. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

136. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

137. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

138. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

139. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

140. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

141. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

142. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

143. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

144. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

145. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

146. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

147. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,

detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

148. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

149. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

150. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Employee Subclass)

151. Plaintiffs and the Employee Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

152. In obtaining employment from Defendant, Plaintiffs and the Employee Subclass provided and entrusted their PII to Defendant.

153. Defendant required Plaintiffs and the Employee Subclass to provide and entrust their PII as condition of obtaining employment from Defendant.

154. As a condition of obtaining employment from Defendant, Plaintiffs and the Employee Subclass provided and entrusted their PII. In so doing, Plaintiffs and the Employee Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiff and the Employee Subclass if their PII had been compromised or stolen.

155. Plaintiffs and the Employee Subclass fully performed their obligations under the implied contracts with Defendant.

156. Defendant breached the implied contracts it made with Plaintiffs and the Employee Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

157. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Employee Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and

impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

158. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Employee Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
VVIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On Behalf of Plaintiff May and the Florida Subclass)

159. Plaintiff May and the Florida Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

160. This cause of action is brought pursuant the FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

161. Defendant's offer, provision, and/or sale of employment or services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

162. Plaintiff May and the Florida Subclass, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

163. Defendant employed or provided services to Plaintiff May and the Florida Subclass.

164. Defendant offered, provided, or sold employment or services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

165. Plaintiff May and the Florida Subclass paid for or otherwise availed themselves and received employment or services from Defendant, primarily for personal, family, or household purposes.

166. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of employment or services to or from Plaintiff May and the Florida Subclass.

167. Defendant's acts, practices, and omissions were done in the course of Defendant's businesses of offering, providing, and servicing loans throughout Florida and the United States.

168. The unfair, unconscionable, and unlawful acts and practices of Defendant alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

169. Defendant, operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that their computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiff May's and the Florida Subclass's PII;

d. continued acceptance and storage of PII after Defendant knew or should have known of the security vulnerabilities that were exploited in the Data Breach;

e. continued acceptance and storage of PII after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

170. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 41, *et seq*., and the FDUTPA, Fla. Stat. § 501.171(2).

171. Defendant knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff May's and the Florida Subclass's PII and that the risk of a data breach or theft was high.

172. Plaintiff May has standing to pursue this claim because as a direct and proximate result of Defendant's violations of the FDUTPA, Plaintiff May and the Florida Subclass have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Defendant's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

173. Plaintiff May also has standing to pursue this claim because, as a direct result of Defendant's knowing violation of the FDUTPA, Plaintiff May is at a substantial present and imminent risk of identity theft. Defendant still possesses Plaintiff May's and the Florida Subclass's PII, and some Plaintiff May's PII has been both accessed and misused by unauthorized third

parties, which is evidence of a substantial and imminent risk of future identity theft for Plaintiff May and the Florida Subclass.

174. Plaintiff May and the Florida Subclass are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendant audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Defendant purge, delete, and destroy PII not necessary for their provisions of services in a reasonably secure manner;

f. ordering that Defendant conduct regular database scans and security checks;

g. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Defendant to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves.

175. Plaintiff May brings this action on behalf of herself and the Florida Subclass for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow employees and consumers to make informed purchasing decisions and to protect Plaintiff May, the Florida Subclass, and the public from Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

176. The above unfair, unconscionable, and unlawful practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff May and the Florida Subclass that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

177. Defendant's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

178. Plaintiff May and the Florida Subclass seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Defendant's actions and/or practices violate the FDUTPA.

179. Plaintiff May and the Florida Subclass are also entitled to recover the costs of this action (including reasonable attorneys' fees) and such other relief as the Court deems just and proper.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

180. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

181. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

182. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

183. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Nationwide Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiffs.

184. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Nationwide Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

185. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. implement an education and training program for appropriate employees regarding cybersecurity.

186. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will

not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

187. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

188. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT V
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

189. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

190. Plaintiffs allege this negligence *per se* theory as alternative to their other negligence claims.

191. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

192. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customer information. The FTC

publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's sensitive PII.

193. Defendant had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and the Class's PII.

194. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein.

195. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

196. Defendant breached its respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's PII.

197. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

198. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

199. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

200. Had Plaintiffs and members of the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

201. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

202. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their personal data, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Five Guys fails to undertake appropriate and adequate measures to protect their personal data in its continued possession.

COUNT VI
VIRGINIA DATA BREACH NOTIFICATION LAW
Virginia Code §§ 18.2-186.6(B)
(On Behalf of Plaintiff Ranck and the Virginia Subclass)

203. Plaintiff Ranck and the Virginia Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

204. Virginia Code § 18.2-186.6(B) requires entities that possess the computerized data of a Virginia resident, including personal information, must disclose without unreasonable delay any breach of its security system upon discovery or notification of the breach. Notice must go to the Office of the Attorney General and any affected Virginia resident.

205. This statute applies to Five Guys because it "maintains computerized data that includes personal information that the individual or entity does not own or license," pursuant to Virginia Code § 18.2-186.6(D).

206. This statute expressly authorizes a Virginia resident to recover direct economic damages.

207. Virginia Code § 18.2-186.6(A) defines "personal information" as "the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number."

208. Plaintiff Ranck's personal information, as defined by Virginia Code § 18.2-186.6(A), including her name and Social Security number, was compromised in the Data Breach.

209. Defendant's Breach Notice was sent at least three months after Five Guy's discovered the Data Breach. This Breach Notice was not timely sent and constitutes unreasonable delay.

210. Plaintiff Ranck has suffered economic injury due to and traceable from the timing of the delayed notification. First, her economic injuries are solely the result of the Data Breach itself. Second, if she had been aware of the Data Breach earlier, she could have taken additional steps to prevent the identity theft that came to pass and the economic injuries arising therefrom.

COUNT VII
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

211. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

212. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

213. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form of disclosing their PII.

214. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs and members of the Class's PII, as this was used to facilitate employment by Defendant.

215. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of the benefits Plaintiffs and the Class conferred because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII had they known Defendant would not adequately protect their PII.

216. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT VIII
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code § 1798.100, *et seq.*
(On behalf of Plaintiff Turner and the California Subclass)

217. Plaintiff Turner and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 121.

218. This Count is brought on behalf of Plaintiff Turner and the California Subclass against Defendant.

219. Defendant violated sections 1798.81.5(b) and 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiff Turner's and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

220. The non-redacted and non-encrypted PII of Plaintiff Turner and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's violations of its duty under the CCPA.

221. Plaintiff Turner and the California Subclass lost money or property, including but not limited to, the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

222. Defendant knew, or should have known, that its network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff Turner and members of the California Subclass was exposed.

a. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff

Turner's and California Subclass' unencrypted first and last names and Social Security numbers among other information.

223. Defendant is organized for the profit or financial benefit of their owners and collect PII as defined in Cal. Civ. Code § 1798.

224. Plaintiff Turner and the California Subclass are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

225. Plaintiff Turner and the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff Turner and the California Subclass. Plaintiff Turner and the California Subclass have an interest in ensuring that their PII is reasonably protected.

226. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Turner gave written notice to Defendant of its specific violations of sections 1798.81.5(b) and 1798.150(a) by email to outside counsel, by agreement, on January 11, 2023.

227. Defendant, however, failed to "actually cure" its violations within 30 days of the written notice, and failed, pursuant to § 1798.150(b) to "provide[] the consumer an express written statement that the violations have been cured and that no further violations shall occur."

228. Defendant failed to "actually cure" its violations by, among other things, not encrypting Plaintiff Turner's and the California Subclass's PII and by not deleting Plaintiff Turner's and the California Subclass's PII it no longer had a reasonable need to maintain in an Internet accessible environment.

229. As a result, Plaintiff Turner and California Subclass members seek relief under § 1798.150(a), including, but not limited to, statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Employee Subclass, the Florida Subclass, the Virginia Subclass, and the California Subclass and appointing Plaintiffs and their Counsel to represent such Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations,

industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals

must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: July 11, 2023

Respectfully Submitted,

/s/ Steven T. Webster

Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington St., Suite 404
Alexandria, VA 22314
(888) 987-9991 (phone and fax)
swebster@websterbook.com

Patrick A. Barthle (*pro hac vice* application forthcoming)
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor

Tampa, Florida 33602
(813) 223-5505
pbarthle@ForThePeople.com

Ryan D. Maxey
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
(813) 448-1125
ryan@maxeyfirm.com

Attorneys for Plaintiff May and the Proposed Class

Raina Borrelli
TURKE & STRAUSS, LLP
613 Williamson Street #201
Madison, WI 53703
Tel: (608) 237-1775
Raina@turkestrauss.com

David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

Attorneys for Plaintiff Ranck and the Proposed Class

M. Anderson Berry
Gregory Haroutunian
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Rachele R. Byrd (*pro hac vice* application forthcoming)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599 / Fax: (619) 234-4599
byrd@whafh.com

Attorneys for Plaintiff Turner and the Proposed Class

Laura Van Note, Esq. (CA S.B. #310160)
Cody Alexander Bolce, Esq. (C.A. S.B. #322725)
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: lvn@colevannote.com
Email: cab@colevannote.com

Attorneys for Plaintiff Thomas and the Proposed Class

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that on July 11, 2023, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

/s/ Steven T. Webster
Steven T. Webster
Webster Book LLP